CyOTE CASE STUDY: NON-MALICIOUS MEMORY EXHAUSTION

SEPTEMBER 23, 2021

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL Idaho National Laboratory

Table of Contents

CyOTE CASE STUDY: NON-MALICIOUS MEMORY EXHAUSTION

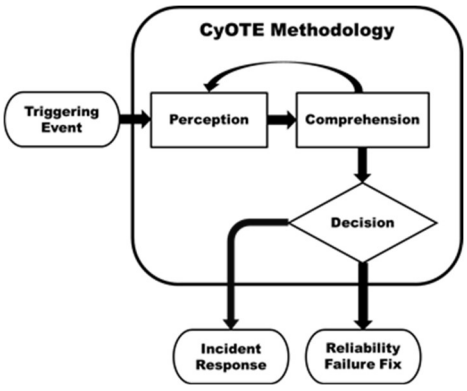
INTRODUCTION

The CyOTE methodology developed capabilities for energy sector asset owners and operators (AOOs) to independently identify adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE), CyOTE is a partnership with energy sector owners and operators. CyOTE seeks to tie effects of a cyber-attack to anomalies—as detected by commercial or in-house solutions—in the OT environment to determine if it has a malicious cyber cause.

Case Studies support continued learning through analysis of incidents and events. Some of the richest and most detailed Case Studies are expected to be produced by AOOs who have employed the CyOTE methodology to perceive and comprehend actual triggering events in their OT environments, with the benefit of complete access to all data and full context. To bootstrap the learning process and complement anticipated AOO-generated Case Studies, the CyOTE team has begun compiling Case Studies of historical OT attacks and OT-related incidents.

This historical Case Study is based on publicly available reports of the incident from media outlets and cybersecurity firms instead of the full context and data that an AOO would have. This Case Study is not, nor is it intended to be, completely comparable in detail or structure, nonetheless it provides examples of how key concepts in the CyOTE methodology look in the real world. Perhaps more importantly, evaluating this historical incident through the CyOTE methodology provides a learning opportunity from the perspective of "how could this have been detected?" instead of "why was this missed?" to grow the body of knowledge on perception, comprehension, and organizational capabilities.

METHODOLOGY



The CyOTE methodology applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. MITRE's ATT&CK® Framework for Industrial Control Systems (ICS)[1] is used as a common lexicon to assess triggering events related to three Use Cases – Alarm Logs, Human-Machine Interface (HMI), and Remote Logins – which together account for 87 percent of the techniques commonly used by adversaries. The CyOTE methodology is also appropriate for OT-related anomalies perceived outside the three Use Cases, such as through the energy delivery system itself.

The Case Study highlights the CyOTE methodology for an AOO to use, starting from the point in time and space an anomalous event or condition meriting investigation – a triggering event – is perceived, and continues to the point where the anomaly is comprehended with sufficient

[1] https://collaborate.mitre.org/attackics/index.php/Main_Page

confidence to make a business risk decision on the appropriate resolution. If sufficient evidence of a malicious nexus is found, then the situation is addressed through existing organizational incident response procedures. Failure to find sufficient evidence of malicious activity defaults to the situation addressed through existing organizational corrective maintenance and work management procedures.

By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables which could represent a faint signal of an attack requiring investigation. CyOTE can assist AOOs in prioritizing their OT environment visibility investments. Over time, AOOs' triggering events will move towards fainter signals, detected earlier, to interdict incidents before more significant harms are realized in the face of infrastructure changes, new technologies, and determined and sophisticated adversaries.

BACKGROUND ON THE ATTACK

The following Case Study is based on events which took place during the September 2020 iteration of the Defense Advanced Research Projects Agency's (DARPA) Rapid Attack Detection, Isolation, and Characterization Systems[2] (RADICS) experiment, conducted with the support of DOE.

The goal of the RADICS program was to enable black start recovery of the power grid amidst a cyber-attack on the U.S. energy sector's critical infrastructure. RADICS research developed technology that cybersecurity personnel, power engineers, and first responders can utilize to accelerate restoration of cyber-impacted electrical systems. Program technologies attempt to accelerate recovery by maintaining situational awareness, enabling network isolation, and rapidly characterizing cyber-attacks. Tools emerging from RADICS research were tested and validated against various threat scenarios in a series of live exercises in a test environment.

The overall RADICS storyline assumes an adversary actively countering AOO efforts to restore power in a blackstart scenario 30 days into a protracted outage. A unique aspect of this Case Study, through experience in RADICS up to this point, participating AOOs were conditioned to presume that most anomalies perceived were due to a cyber threat in the experiment, instead of collecting information and analyzing the situation to determine a likely cause. This scenario event did not directly affect any specific participant.

SCENARIO DESCRIPTION

In the RADICS exercise, the control center experiences a loss of communication with the substation automation controller in the substation. A field operator is dispatched to the substation to power cycle the substation automation controller. When automation controller communication is not restored upon restart, a technician is dispatched to the substation to investigate. Following seven different threads of troubleshooting, the AOO was able to rule out potential use of eighteen adversary techniques with sufficient confidence to decide that the loss of communications was a reliability failure and not the result of malicious cyber activity. At this point, an onsite device OEM representative was brought in and determined that the device had lost communications because its memory was full due to a failure of the local log rotation routine.

[2] https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

The AOO had focused its troubleshooting on the communications path instead of the device, likely lengthening the time required to reach a decision on response actions. Forensic analysis by the OEM determined that a software update some time ago had been unsuccessful, and resulted in a specific log file ceasing to rotate once it exceeded a certain file size; because this log file is infrequently written to it had taken several months for the non-rotating log file to grow large enough to consume all the storage on the device.

In the exercise, the following data sources were investigated for the purposes of applying the CyOTE methodology as discussed below.

Triggering Events: Loss of communications with automation controller, communication not restored upon restart.

Observables**:** Loss of control, loss of view

Use Cases: HMI, Alarm Logs, Remote Login

Data Sources: Network captures

MAP OF POTENTIAL ATTACK TTPS

For the CyOTE methodology to succeed, sufficient data is needed, as is further investigation. From the three Use Cases, techniques were identified that could be responsible for the observable (loss of communication combined with power cycle not restored). By mapping the potential techniques, tactics, and procedures an attacker may have used to gain access, CyOTE researchers can connect the dots to reveal attacker activity. AOOs can utilize this information in their own environments to quickly identify potential attacks and take mitigative actions.

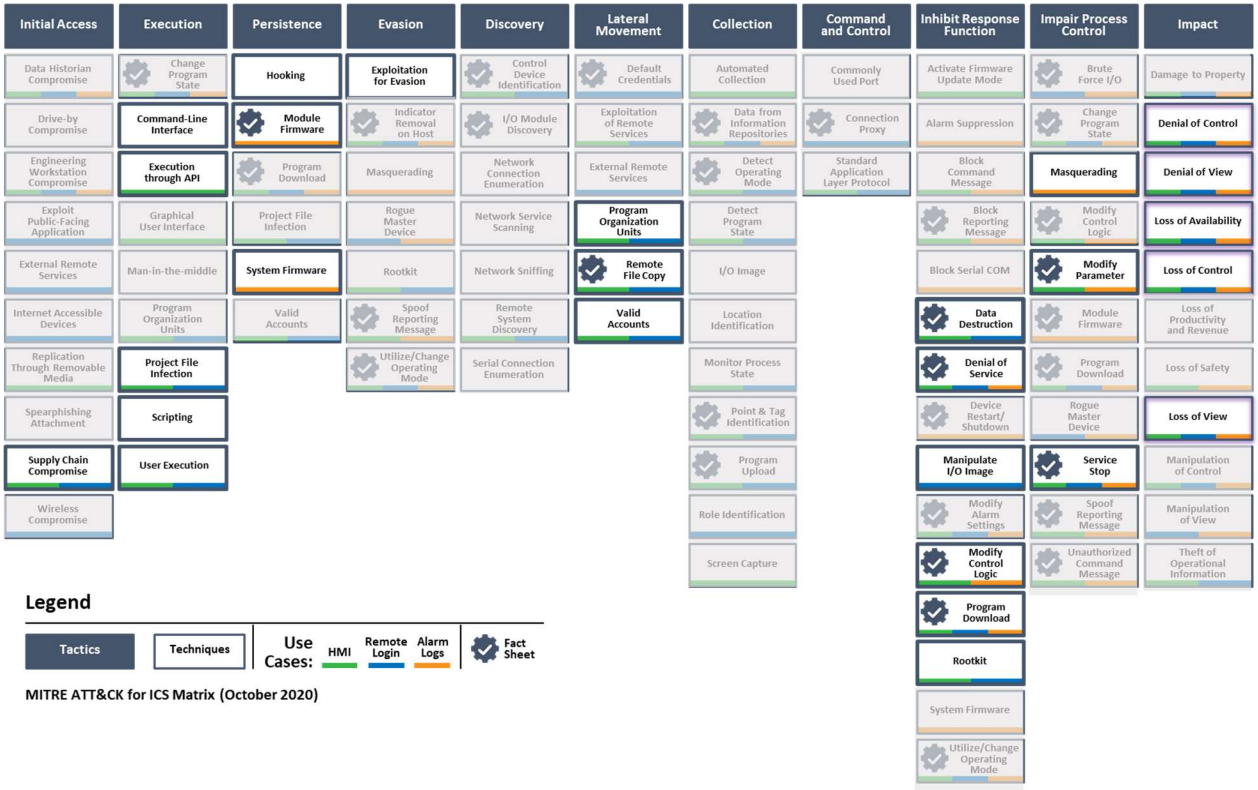


Figure 1. RADICS Blackstart Scenario Potential Adversary Techniques

APPLICATION OF THE CyOTE METHODOLOGY AND TECHNIQUES

Using available data, researchers looked for evidence of potential techniques to identify a path that would demonstrate that the observable was the result of a cyber-attack.

1. Perception – Potential Techniques:
   - Remote File Copy (T867)
   - Program Organization Units (T844)
   - Project File Infection (T873)
   - Manipulate I/O Image (T835)
   - Modify Control Logic (T833)
   - Program Download (T843)
   - Module Firmware (T839)
   - System Firmware (T857)

   Comprehension Opportunities: These techniques all require file uploads, evidence of which could be seen through packet capture analysis and possibly through SIEM capabilities. Here, inspection of Network captures (SIEM; Zeek; Raw Pcap; etc.) returned no evidence of file uploads.

2. Perception – Potential Technique: Valid Accounts (T859)

   Comprehension Opportunities: Reviewing logins for irregularities of user, system, location, time and duration could provide evidence of inappropriate use of valid credentials. Here, no unusual login attempts were detected.

3. Perception – Potential Technique: User Execution (T863)

   Comprehension Opportunities: Inspection of physical access logs and network traffic, including web interface traffic, commands which are indicative of user interaction, and traffic authenticated as a user could provide evidence of user execution. Here, no abnormal traffic was identified for user action.

4. Perception – Potential Technique: Modify Parameter (T836)

   Comprehension Opportunities: Application layer packets containing device command messages could provide evidence of parameter modification. Here, network traffic inspection and looking within (layer 7) packets revealed no command messages which modified parameters.

5. Perception – Potential Technique: Execution through API (T871)

   Comprehension Opportunities: In the context of the experiment environment, abnormal or unauthorized API usage detected in network traffic associated with recent technician access to the suspect device could provide evidence of API execution. Here, inspection of network captures revealed evidence of recent technician access, but no additional abnormal or unauthorized API usage was detected.

6. Perception – Potential Techniques:
   - Command Line Interface (T807)

- Scripting (T853)
- Data Destruction (T809)
- Denial of Service (T814)
- Service Stop (T881)
- Masquerading (T849)

Comprehension Opportunities: In the context of the experiment environment, cooperation with the AOO's vendors who have remote access capabilities could provide evidence of these techniques.

7. Perception – Potential Techniques:

   - Supply Chain Compromise (T862)
   - Hooking (T874)
   - Exploitation for Evasion (T820)
   - Rootkit (T851)

   Comprehension Opportunities: Deeper forensic inspection of implicated devices after removal from service could provide evidence of these techniques.

Having discredited the above techniques in the potential attack path, a vendor onsite was called in to bypass normal login procedures and further diagnose the device. This diagnosis determined that storage was full and that local log rotation was failing, determining the cause of device unresponsiveness, but not the cause of log filling.

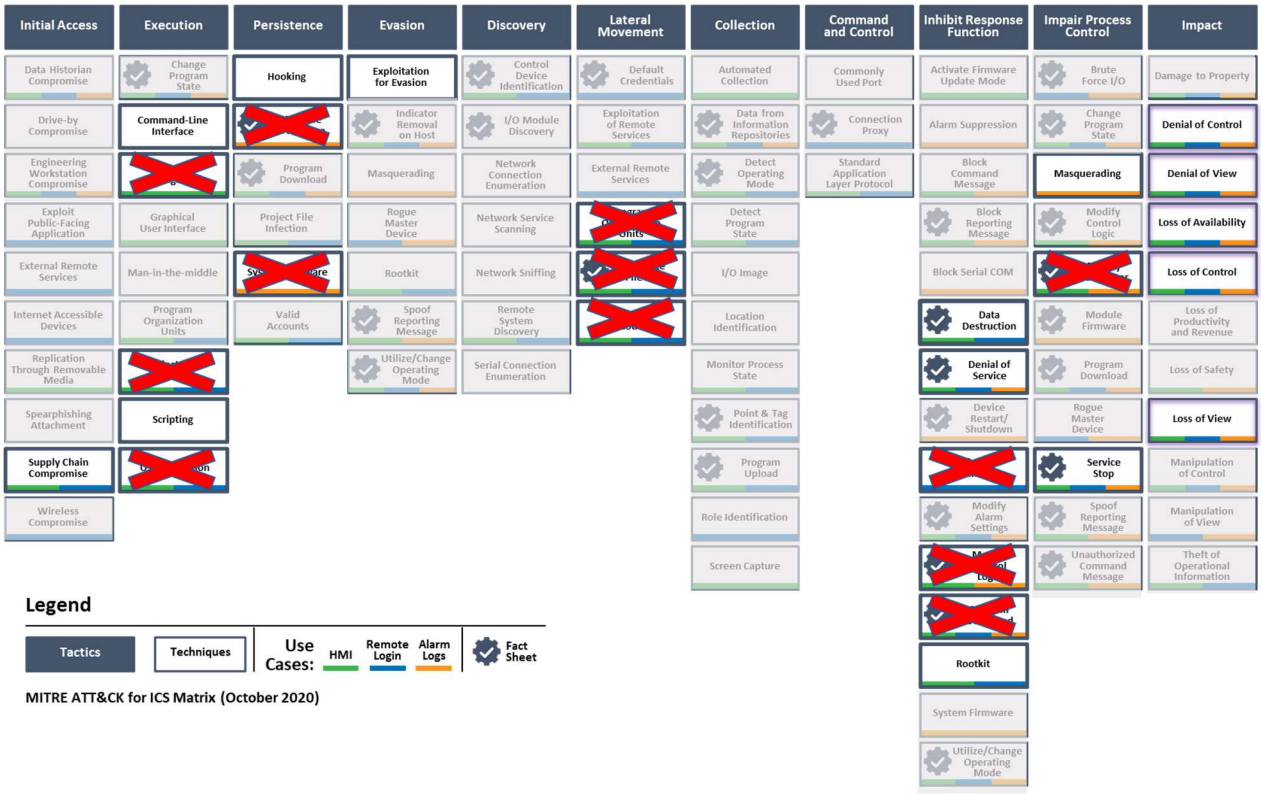


Figure 2. RADICS Blackstart Scenario Potential Adversary Techniques Eliminated

With all available data assessed, no evidence of TTPs was found, but some techniques were not explicitly disproven either. Here, the CyOTE methodology returns to the map to look for an attack path across the remaining techniques. Figure 2 demonstrates a clear absence of a possible attack path across the remaining potential TTPs, meaning that this incident could be viewed as a non-cyber event.

DECISION: RELIABILITY FAILURE

A failed update to the system caused the log rotation on the system to fail. This led to a specific log on the system to not be rotated once it reached a specific size. This log file was infrequently written to and took months to fill the storage on the device. The no disk storage message can manifest itself in different ways, including the inability to log in, individual service degradation, up to device failure. It was therefore concluded that this was not a cyber-event, but in reality a device failure.

CONCLUSION

The Non-Malicious Memory Exhaustion Case Study demonstrates how the CyOTE methodology can be employed in a high-pressure situation to determine if a failure or anomaly is part of an attack underway. Once a triggering event occurs, an AOO can conduct investigation, stringing together potential techniques within relevant use cases and tying them to observables that have occurred in the OT environment to establish a chain of events. Unmasking the presence or absence of an attack path can inform decision making so that the best resources are deployed to resolve the failure—whether that be a maintenance team or cyber incident response team.

SCENARIO CONSIDERATIONS FOR AOOs USING CyOTE CASE STUDIES

After reviewing this Case Study, AOOs should consider how a similar scenario could unfold in their operating environment, determine the level and location of visibility necessary for them to perceive the triggering event and other anomalies, and identify accessible information sources to build comprehension. The following questions for reflection and discussion can help AOOs prepare to employ the CyOTE methodology in their organization.

- Could you perceive a similar triggering event in your organization? How would it be perceived, and by whom?
- What observables exist that could have been perceived earlier than the triggering event was? How would each be perceived, and by whom?
- Who will you contact from the System Operations, Engineering, and Cybersecurity departments to build comprehension? Would they be willing and able to assist today?
- How much evidence would you need to confidently reject the null hypothesis of a reliability failure, and initiate cybersecurity incident response procedures?
- Who else in your organization needs to be aware of the outcome?

AOOs can refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557